10/521671

Fig.1

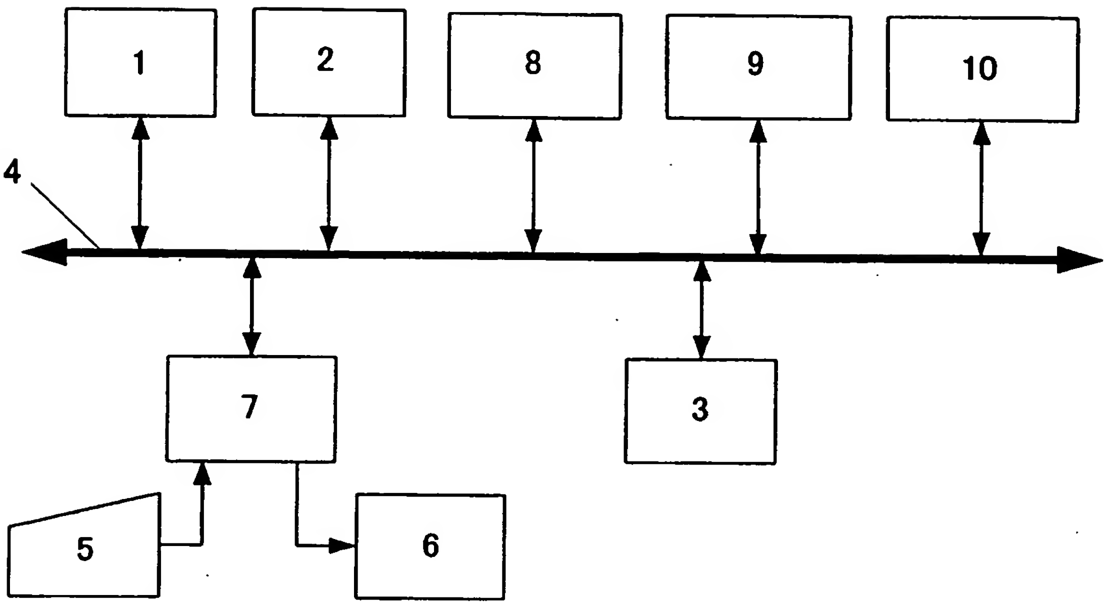
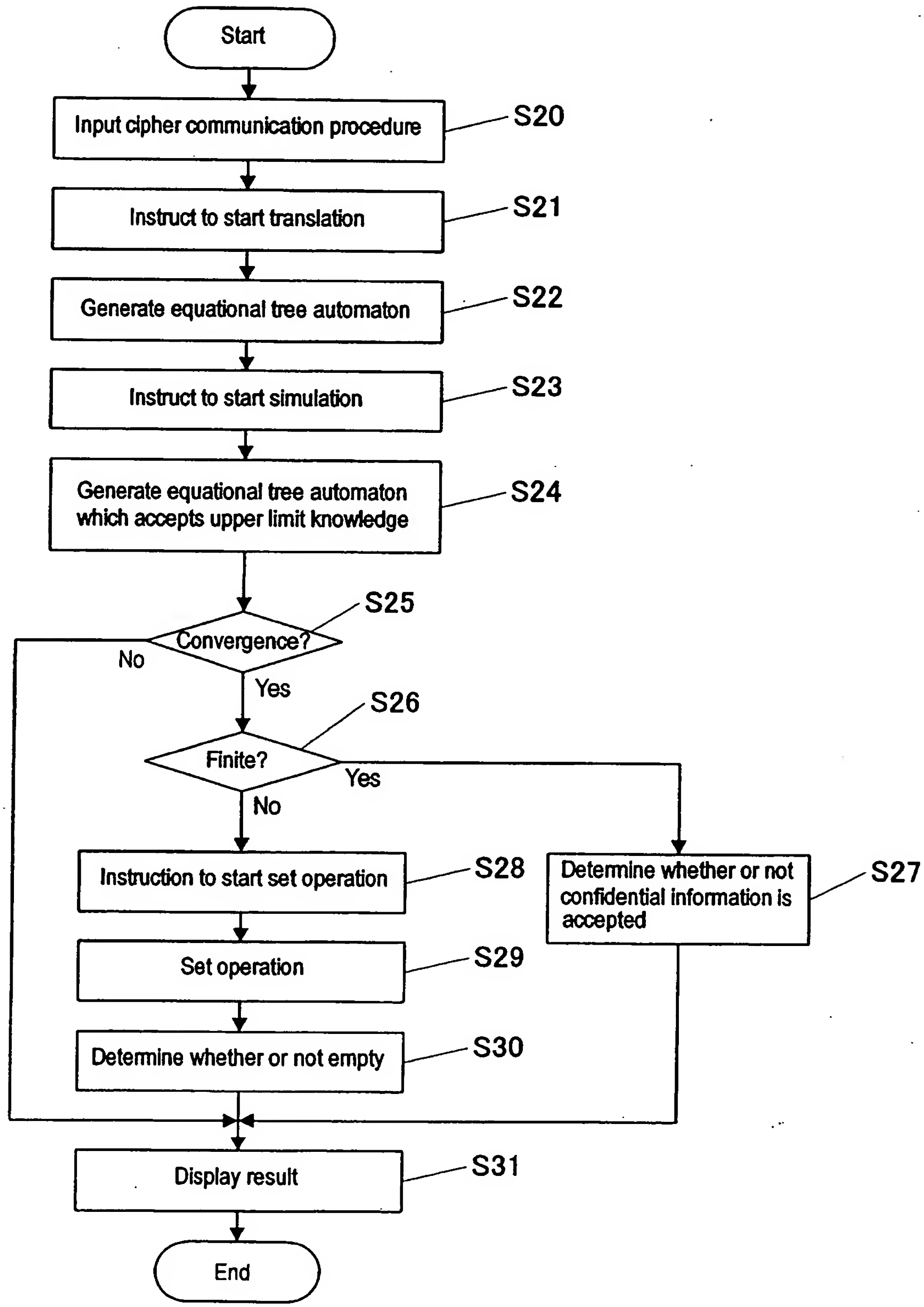


Fig.2



Start
Input cipher communication procedure
S20
Instruct to start translation
S21
Generate equational tree automaton
S22
Instruct to start simulation
S23
Generate equational tree automaton which accepts upper limit knowledge
S24
Convergence?
S25
No
Yes
Finite?
S26
Yes
No
Instruction to start set operation
S28
Determine whether or not confidential information is accepted
S27
Set operation
S29
Determine whether or not empty
S30
Display result
S31
End

Fig.3

Designate input/output argument

Input $l \rightarrow r$: Rewriting rule

$\mathcal{A}/\mathsf{AC}$: Equational tree automaton

Output $\mathcal{B}_{l\rightarrow r}/\mathsf{AC}$: Equational tree automaton

Initial setting

$\mathcal{A}_0 := \mathcal{A};\ i := 0;\ j := 0;$

$S := \mathsf{pos}(l);$

$T := \mathsf{pos}(r);$

First process

while $S \neq \varnothing$ do

Select element p which satisfies the following condition from S : $\forall p' \in S.\ p \succeq p'$

Calculate equational tree automaton $\mathcal{A}_{i+1}/\mathsf{AC}$ which satisfies the following condition : · · · (1)

when $l_{|p} = f(t_1, \ldots, t_n)$

$$\mathcal{L}(\mathcal{A}_{i+1}/\mathsf{AC}) = (\{\rightarrow_{\{f(c_{t_1}^{p\cdot 1},\ldots,c_{t_n}^{p\cdot n})\rightarrow c_{l_{|p}}^{p}\}/\mathsf{AC}})[\mathcal{L}(\mathcal{A}_i/\mathsf{AC})]$$

$i := i+1;$

$S := S - \{p\};$

od

Calculate equational tree automaton $\mathcal{B}_0/\mathsf{AC}$ which satisfies the following condition

$$\mathcal{L}(\mathcal{B}_0/\mathsf{AC}) = (\{\rightarrow_{\{c_l^{\epsilon}\rightarrow d_r^{\epsilon}\}/\mathsf{AC}})[\mathcal{L}(\mathcal{A}_i/\mathsf{AC})]$$

Second process

while $T \neq \varnothing$ do

Select element q which satisfies the following condition from T : $\forall q' \in T.\ q' \succeq q$

Calculate equational tree automaton $\mathcal{B}_{j+1}/\mathsf{AC}$ which satisfies the following condition : · · · (2)

when $r_{|q} = f(t_1, \ldots, t_n)$

$$\mathcal{L}(\mathcal{B}_{j+1}/\mathsf{AC}) = (\{\rightarrow_{\{d_{r_{|q}}^{q}\rightarrow f(d_{t_1}^{q\cdot 1},\ldots,d_{t_n}^{q\cdot n})\}/\mathsf{AC}})[\mathcal{L}(\mathcal{B}_j/\mathsf{AC})]$$

$j := j+1;$

$T := T - \{q\};$

od

$\mathcal{B}_{l\rightarrow r} := \mathcal{B}_j;$

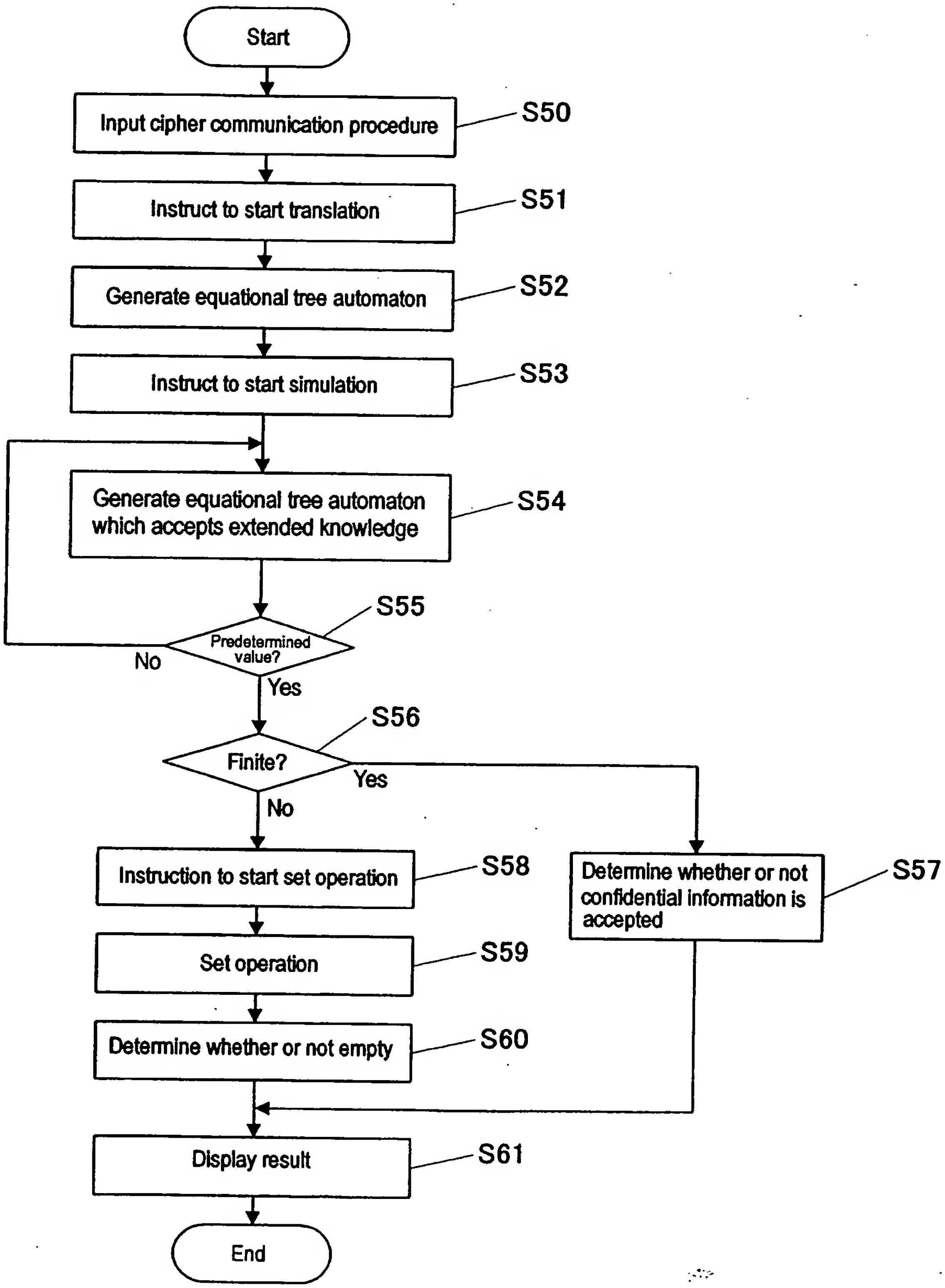
return $\mathcal{B}_{l\rightarrow r}/\mathsf{AC}$

10/521671

Fig.4

Set	Transition rule	Condition
$\mathcal{R}_{\times}$	$f((p_1,q_1),\ldots,(p_n,q_n)) \to (p,q)$	$\forall f \in \mathcal{F} \setminus \mathcal{G}$ $\forall f(p_1,\ldots,p_n) \to p \in \mathcal{R}_{\mathcal{A}}$ $\forall f(q_1,\ldots,q_n) \to q \in \mathcal{R}_{\mathcal{B}}$
$\mathcal{R}_{\overline{\mathcal{A}}}$	$g((p_1,q_1),(p_2,q_2)) \to g((p,q_1),q_2)$ $g(p_1,(p_2,q_2)) \to (p,q_2)$	$\forall g \in \mathcal{G}$ $\forall q_1,q_2 \in \mathcal{Q}_{\mathcal{B}}$ $\forall g(p_1,p_2) \to p \in \mathcal{R}_{\mathcal{A}}$
	$g((p_1,q_1),(p_2,q_2)) \to g((r_1,q_1),(r_2,q_2))$ $g(p_1,(p_2,q_2)) \to g(r_1,(r_2,q_2))$	$\forall g(p_1,p_2) \to g(r_1,r_2) \in \mathcal{R}_{\mathcal{A}}$
$\mathcal{R}_{\overline{\mathcal{B}}}$	$g((p_1,q_1),(p_2,q_2)) \to g((p_1,q),p_2)$ $g(q_1,(p_2,q_2)) \to (p_2,q)$	$\forall g \in \mathcal{G}$ $\forall p_1,p_2 \in \mathcal{Q}_{\mathcal{A}}$ $\forall g(q_1,q_2) \to q \in \mathcal{R}_{\mathcal{B}}$
	$g((p_1,q_1),(p_2,q_2)) \to g((p_1,r_1),(p_2,r_2))$ $g(q_1,(p_2,q_2)) \to g(r_1,(p_2,r_2))$	$\forall g(q_1,q_2) \to g(r_1,r_2) \in \mathcal{R}_{\mathcal{B}}$
$\mathcal{R}_{\mathcal{G}}$	$g((p,q_1),q_2) \to g(q_1,(p,q_2))$ $g((p_1,q),p_2) \to g(p_1,(p_2,q))$ $g(q,p) \to (p,q)$	$\forall g \in \mathcal{G}$ $\forall p_1,p_2,p \in \mathcal{Q}_{\mathcal{A}}$ $\forall q_1,q_2,q \in \mathcal{Q}_{\mathcal{B}}$

Fig.5


Start
Input cipher communication procedure
S50
Instruct to start translation
S51
Generate equational tree automaton
S52
Instruct to start simulation
S53
Generate equational tree automaton which accepts extended knowledge
S54
Predetermined value?
S55
No
Yes
Finite?
S56
Yes
No
Instruction to start set operation
S58
Determine whether or not confidential information is accepted
S57
Set operation
S59
Determine whether or not empty
S60
Display result
S61
End